SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

SPYWOLF

Security Audit Report

Audit prepared for

Monstro's Degenz

Completed on

December 20, 2023

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

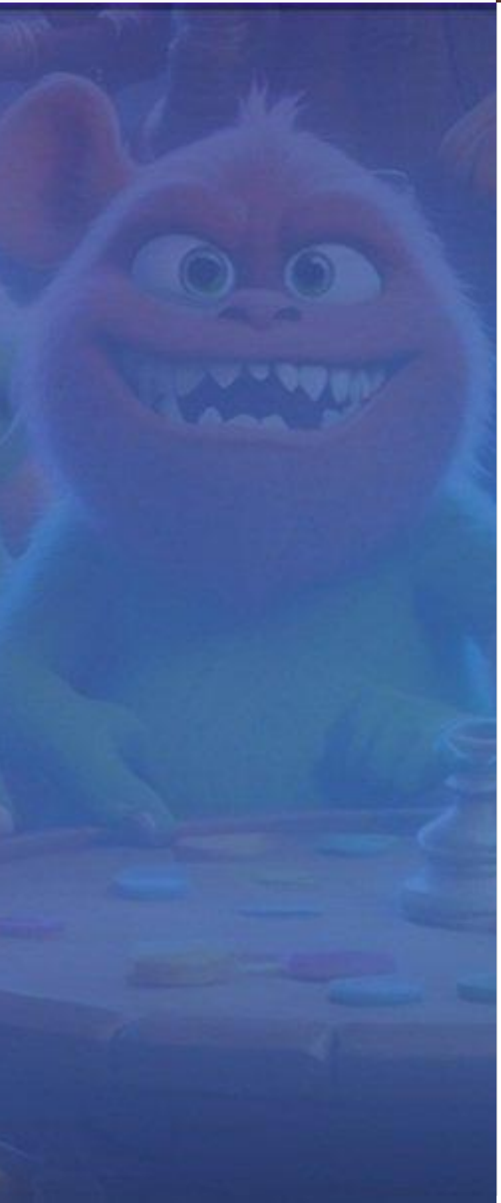
You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

Monstro's Degenz



PROJECT DESCRIPTION

According to their whitepaper:
"Are you a DeFi enthusiast who loves the allure of profitable ROI dApps but hates enduring endless losses? Look no further than Monstro's Degenz! Unleash your inner degen amongst the safety of your fellow monsters."

Release Date: December 27th, 2023

Category: ROI dApp, Farming

CONTRACT INFO

Token Name	MonstroDegenzS1	Symbol	N/A
Contract Address	0xCc57F57e82D8A96Ef488D150f5A7fB11882d1176		
Network	Binance Smart Chain	Language	Solidity
Deployment Date	Dec 18, 2023	Contract Type	Staking
Total Supply	N/A	Status	Launched

TAXES

Buy Tax	Sell Tax
***30% + ref reward**	**5%**

***Distribution of buy tax according to the project's team: "Farmz working capital, which benefits the user as it is their "safety net" passive income for when the "ROI dApp" phase runs dry." Referral reward tax can be up to 20%, depending on referral's cashback settings.**

For more information check their documents page:
https://wiki.monstro.fun/universe/

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	N/A
Uniq Senders	N/A
Uniq Receivers	N/A
Total Amount	N/A
Median Transfer Amount	N/A
Average Transfer Amount	N/A
First transfer date	N/A
Last transfer date	N/A
Days token transferred	N/A

SMART CONTRACT STATS

Calls Count	2
External calls	2
Internal calls	0
Transactions count	2
Uniq Callers	1
Days contract called	1
Last transaction time	2023-12-18 04:19:34 UTC
Created	2023-12-18 04:14:10 UTC
Create TX	0x9e9a2d1e37c49370b628f8b300d85fdff9b5c68f03865747fcce8810616b7de8
Creator	0xcc4c5217bdf5a4fec38476531bd4546cbc306290

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

No high risk-level threats found in this contract.

⚠ Medium Risk

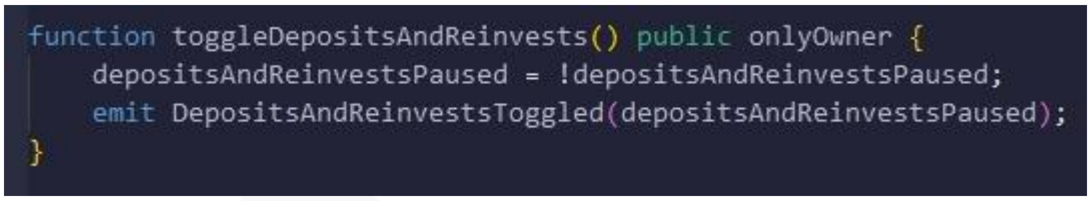
No medium risk-level threats found in this contract.

⚠ Low Risk

No low risk-level threats found in this contract.

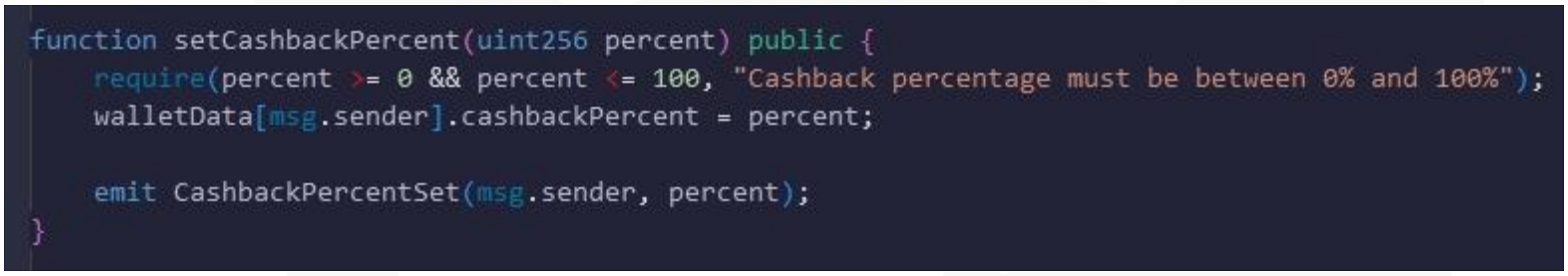
Informational

Owner can stop new deposits and reinvestments, but cannot stop rewards claiming.



```
function toggleDepositsAndReinvests() public onlyOwner {
    depositsAndReinvestsPaused = !depositsAndReinvestsPaused;
    emit DepositsAndReinvestsToggled(depositsAndReinvestsPaused);
}
```

Users can set cashback percent for their referrals up to 100%.



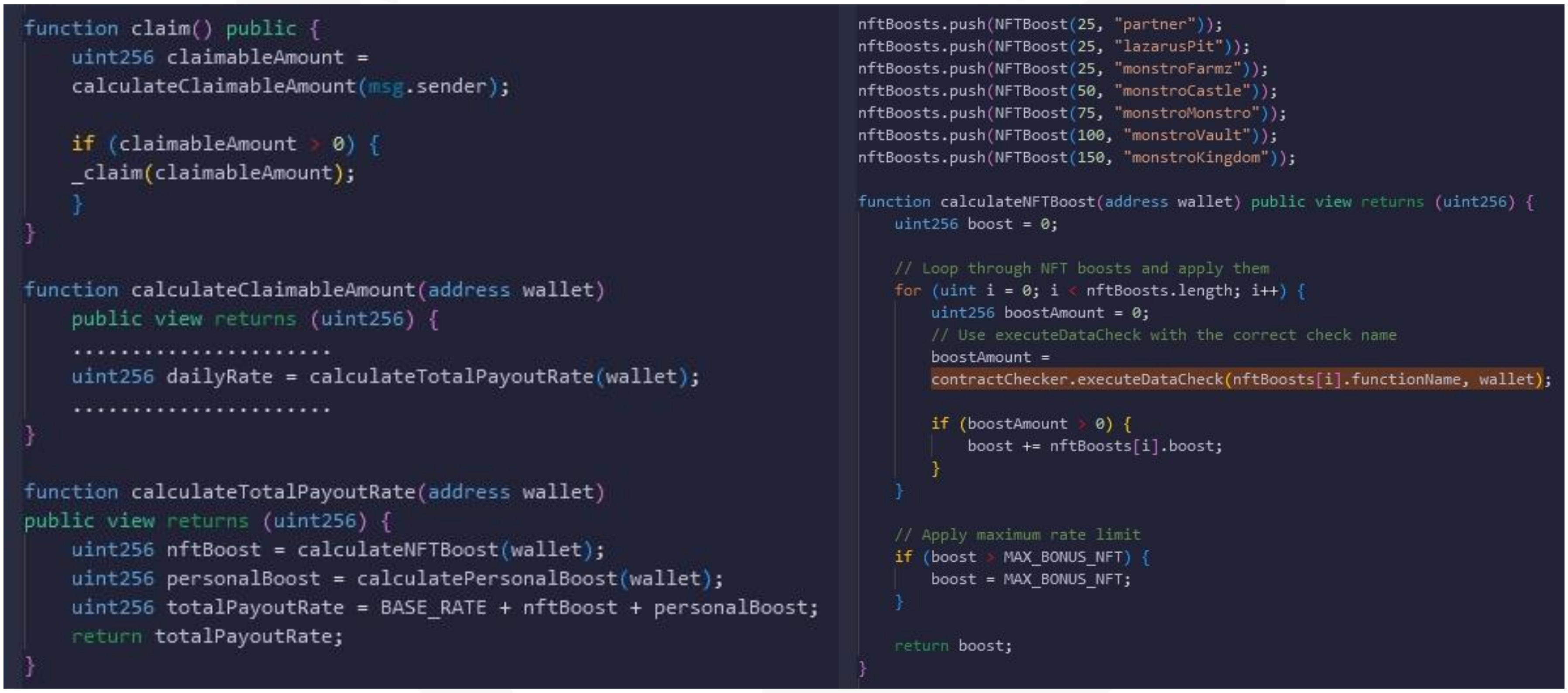
```
function setCashbackPercent(uint256 percent) public {
    require(percent >= 0 && percent <= 100, "Cashback percentage must be between 0% and 100%");
    walletData[msg.sender].cashbackPercent = percent;

    emit CashbackPercentSet(msg.sender, percent);
}
```

Informational

NFT boost check data is taken from external contract which is **not** part of the current audit. NFT boost can be up to 2%.

In the current contract architecture, the external contract is used to communicate with set of NFT contracts and deliver proper data. Adding/removing function calls in the external contract should be handled with care by the owners.
If external contract’s function is paused and/or set to return inappropriate data, this will reflect the current staking contract as well and claim functionality may halt.



```
function claim() public {
    uint256 claimableAmount =
    calculateClaimableAmount(msg.sender);

    if (claimableAmount > 0) {
    _claim(claimableAmount);
    }
}

function calculateClaimableAmount(address wallet)
    public view returns (uint256) {
    ......................
    uint256 dailyRate = calculateTotalPayoutRate(wallet);
    ......................
}

function calculateTotalPayoutRate(address wallet)
public view returns (uint256) {
    uint256 nftBoost = calculateNFTBoost(wallet);
    uint256 personalBoost = calculatePersonalBoost(wallet);
    uint256 totalPayoutRate = BASE_RATE + nftBoost + personalBoost;
    return totalPayoutRate;
}
```

```
nftBoosts.push(NFTBoost(25, "partner"));
nftBoosts.push(NFTBoost(25, "lazarusPit"));
nftBoosts.push(NFTBoost(25, "monstroFarmz"));
nftBoosts.push(NFTBoost(50, "monstroCastle"));
nftBoosts.push(NFTBoost(75, "monstroMonstro"));
nftBoosts.push(NFTBoost(100, "monstroVault"));
nftBoosts.push(NFTBoost(150, "monstroKingdom"));

function calculateNFTBoost(address wallet) public view returns (uint256) {
    uint256 boost = 0;

    // Loop through NFT boosts and apply them
    for (uint i = 0; i < nftBoosts.length; i++) {
        uint256 boostAmount = 0;
        // Use executeDataCheck with the correct check name
        boostAmount =
        contractChecker.executeDataCheck(nftBoosts[i].functionName, wallet);

        if (boostAmount > 0) {
            boost += nftBoosts[i].boost;
        }
    }

    // Apply maximum rate limit
    if (boost > MAX_BONUS_NFT) {
        boost = MAX_BONUS_NFT;
    }

    return boost;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Monstro's Degenz

GOOD PRACTICES FOUND

✓ The owner cannot set a transaction limit

TOKENOMICS

This is a ROI dApp offering daily ROI of 2% to 6%. Users can increase their daily ROI through NFT and Personal "boosts". Base rate is 2%, NFT bonuses up to 2% and deposit value bonuses up to 2% allow for a total of 6% daily ROI.

Deposited funds are allocated as follows:
50% - Liquidity
30% - Farmz! working capital (on user's behalf)
20% - Referrals & Marketing

Claims are subject to a 5% tax:
4% - Team
1% - Genesis NFT holders

There is an aggressive referral program with rewards ranging from 5% - 20% based on total referred volume. Affiliates may also set a cashback % (up to 100%) to share rewards with their referrals. All rewards are paid out instantly in BNB.

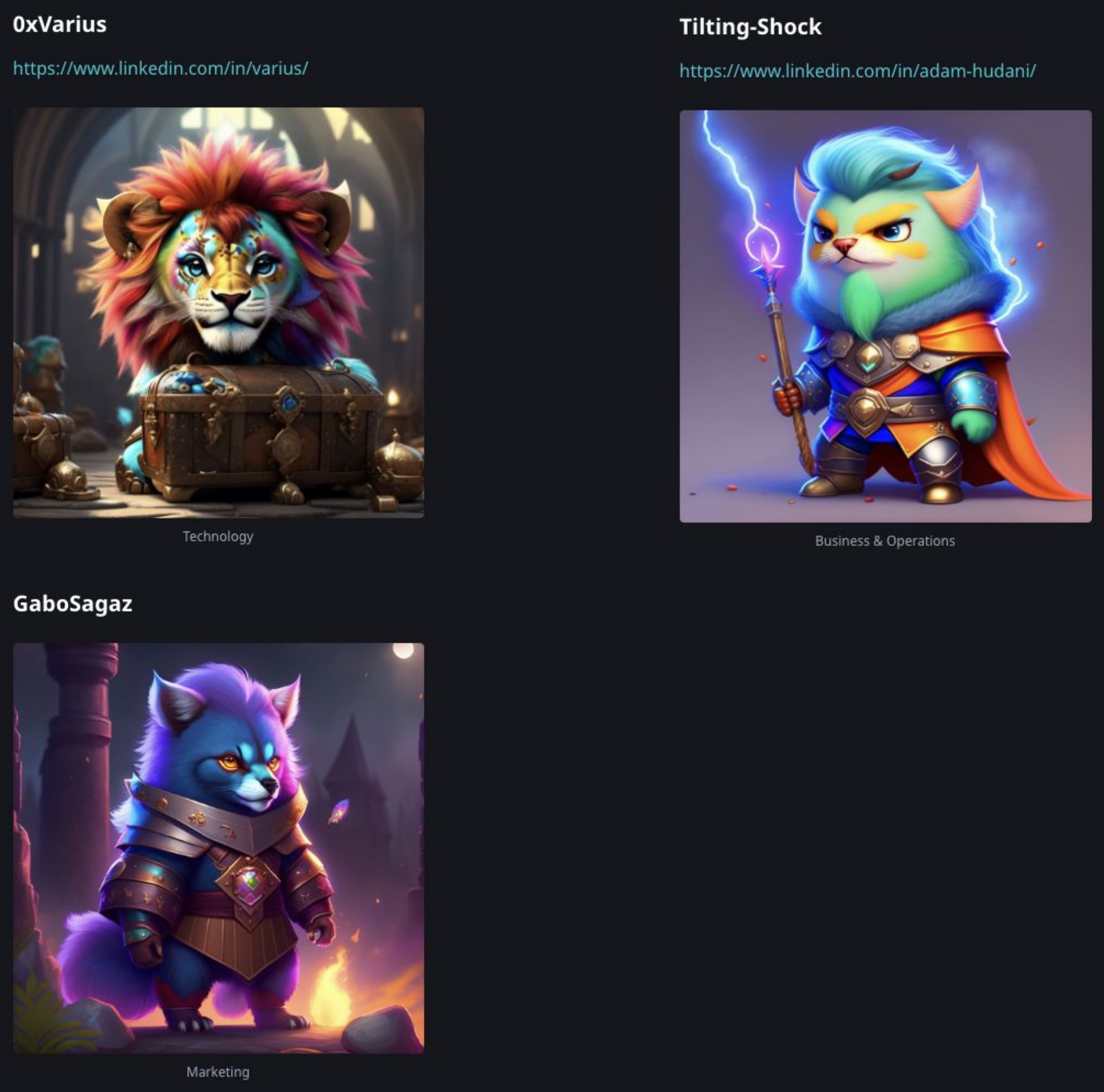
"No Lose" Guarantee
Given ROI dApps are typically volatile and considered high-risk, Degenz! differentiates itself by offering a "safety net" in the form of weekly passive income through yield farming. Working capital for farming is collected on every deposit and reinvestment.

ROI - *Return of investment*

ROI dapps are usually subject to high volatility and considered as high risk investments.

THE TEAM

✅ The team at Monstro is well-known and publicly doxxed. Linkedin profiles were provided.



0xVarius

https://www.linkedin.com/in/varius/

Technology

Tilting-Shock

https://www.linkedin.com/in/adam-hudani/

Business & Operations

GaboSagaz

Marketing

WEBSITE

Home Website URL
https://monstro.fun/

Domain Registry
https://namecheap.com

Domain Expiration
2024-04-20

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

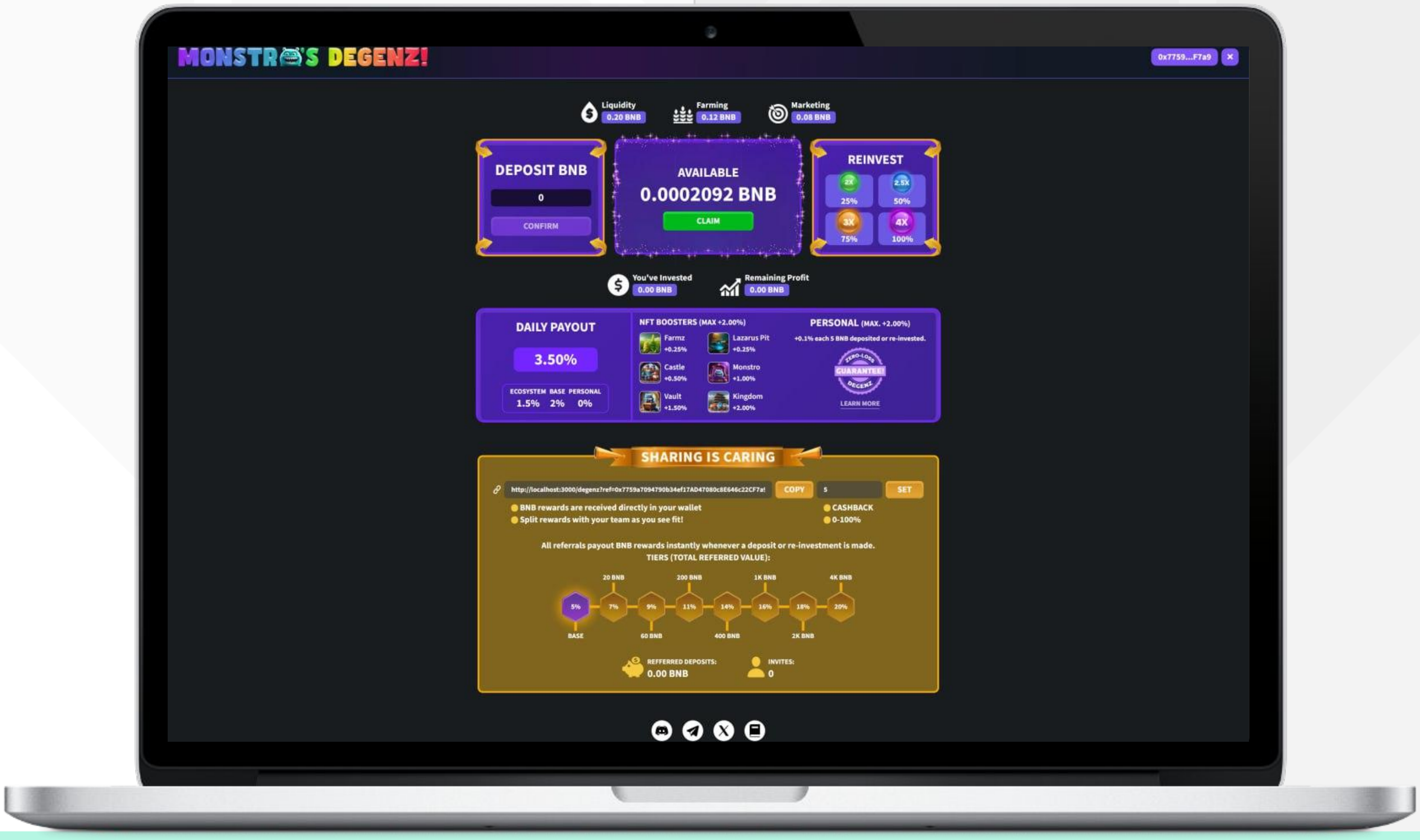
Design
Very nice color scheme and overall layout.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written and explanatory documents page

Roadmap
Yes, goals set

Mobile-friendly?
Yes



+0.1% each 5 BNB deposited or re-invested.

http://localhost:3000/degenz?ref=0x7759a7094790b34ef17AD47080c8E646c22CF7a!

- BNB rewards are received directly in your wallet
- Split rewards with your team as you see fit!

All referrals payout BNB rewards instantly whenever a deposit or re-investment is made.
TIERS (TOTAL REFERRED VALUE):

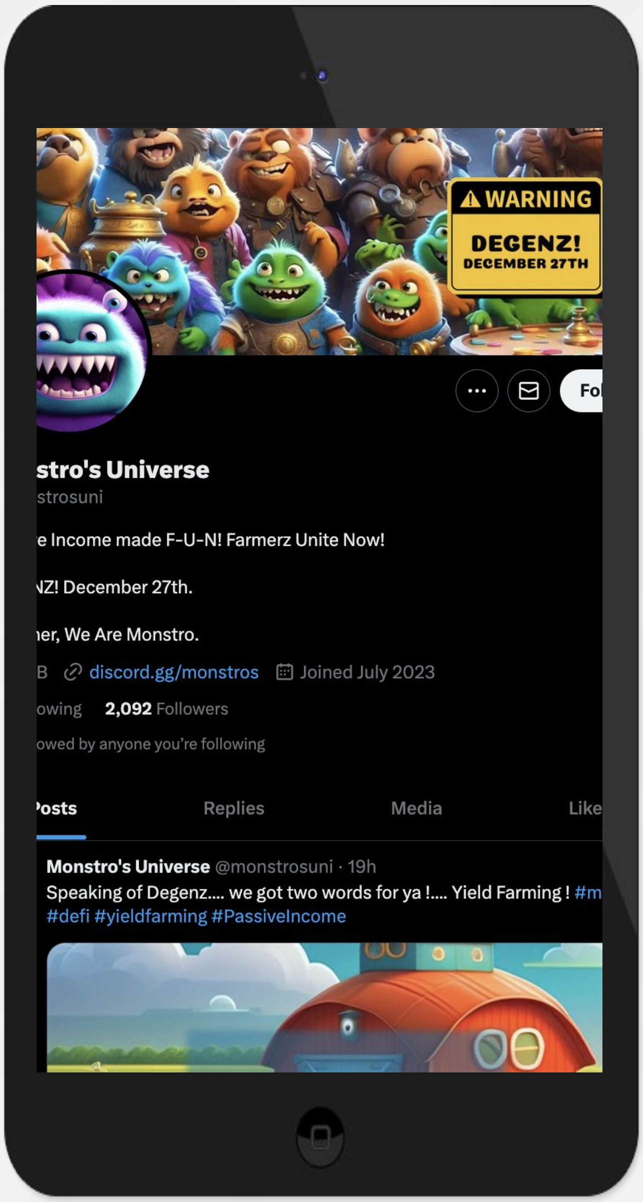
monstro.fun/degenz

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are very active with devs and users interacting often.



stro's Universe
strosuni

e Income made F-U-N! Farmerz Unite Now!

NZ! December 27th.

ner, We Are Monstro.

B discord.gg/monstros Joined July 2023

owing 2,092 Followers

owed by anyone you're following

Monstro's Universe @monstrosuni · 19h
Speaking of Degenz.... we got two words for ya !.... Yield Farming ! #m
#defi #yieldfarming #PassiveIncome

Twitter

@monstrosuni

- 2 092 followers
- Active
- Posts frequently

Discord

@monstros

- 1718 members
- Active community

Telegram

@monstrosU

- 232 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 700 SUCCESSFUL CLIENTS
- ✓ MORE THAN 1000 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.